Azure-arkkitehtuuri ja -määritykset

Oulun Digi

6.6.2019 / 1.0

Versiotiedot

Versio	Pvm	Tekijä	Huomautuksia
0.5	11.11.2016		Ensimmäinen versio
0.6	16.11.2016		Päivitetty Site REcoveryn kokoonpanoa
0.7	3.12.2016		Toisen Oulu-workshopin jälkeiset päivitykset
0.8	7.1.2017		Versio Oukan kommentteja varten
	14.1.2017		Päivitetty Site Recovery -kohtaa
0.9	6.6.2019	Jussi Tarkkonen / Microsoft	Muokattu Uusien tilauksien osuutta

Sisällysluettelo

1 Johdanto

Tässä dokumentissa kuvataan Oulun kaupungin Azure-ympäristön arkkitehtuuri ja ympäristöön tehdyt määritykset. Azure-ympäristön on pystytetty Oulun Digin toimesta, ja Digi hallitsee ympäristöä. Jäljempänä tässä dokumentissa Oulun kaupungista käytetään lyhennystä Ouka, ja Oulun Digistä käytetään lyhennystä Digi.

Dokumentissa kuvattua ympäristöä on tarkoitus käyttää Oulun kaupungin ja Digi:n asiakasorganisaatioiden palvelimien ylläpitämiseen. Asiakasorganisaatioista käytetään jatkossa termiä asiakasorganisaatio tai asiakas.

Dokumenttiin on lisätty myös Sovelluskohtaiset tarpeet ja muutettu alkuperäistä arkkitehtuuria niin että Sovellukset voi käyttää Oulun Kaupungin kapasiteettia Azuresta.

2 Azure-tilaukset

Oukan Azure-ympäristöön on pystytetty kaksi tuotantotilausta. Jatkossa on tarkoitus, että kaikki tuotannossa olevat, Azureen siirretyt palvelut sijoitetaan Azure-tuotantotilaukseen, ja testausta ja kehitystä varten pystytetään tarvittaessa omia tilauksia.

Tilausten perustamista varten on perustettu erillinen Azure AD -tunnus, jota on tarkoitus käyttää kaikkien tilausten perustamiseen:

- Tunnus: xxx

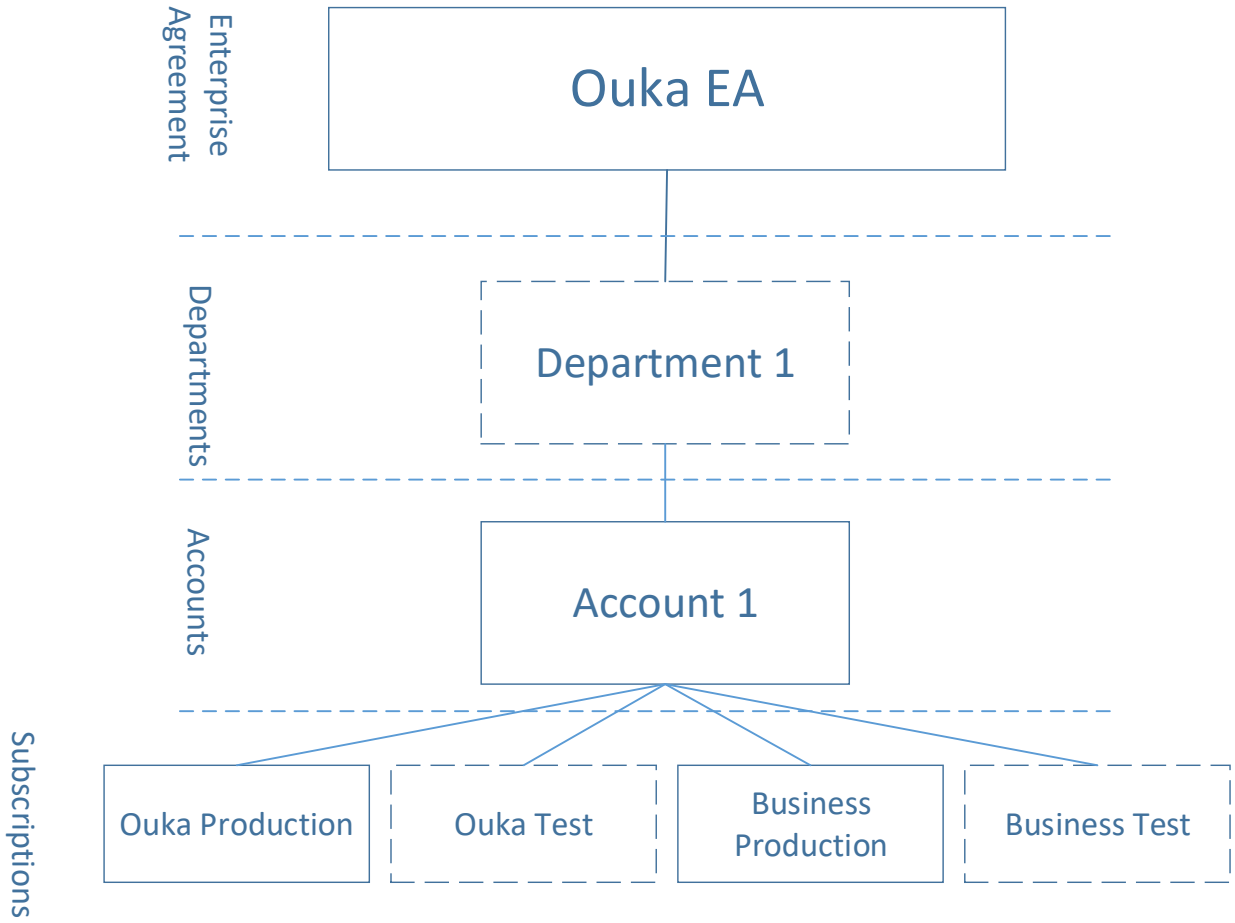
Tunnuksen salasana on digillä tallessa.

Kaikkiin tilauksiin on liitetty ja liitetään Oulun kaupungin Azure AD -hakemisto:

- Hakemisto: Oulun kaupunki / Oulun Tietotekniikka Liikelaitos
- Tenant-tunnus: oulunkaupunki.onmicrosoft.com

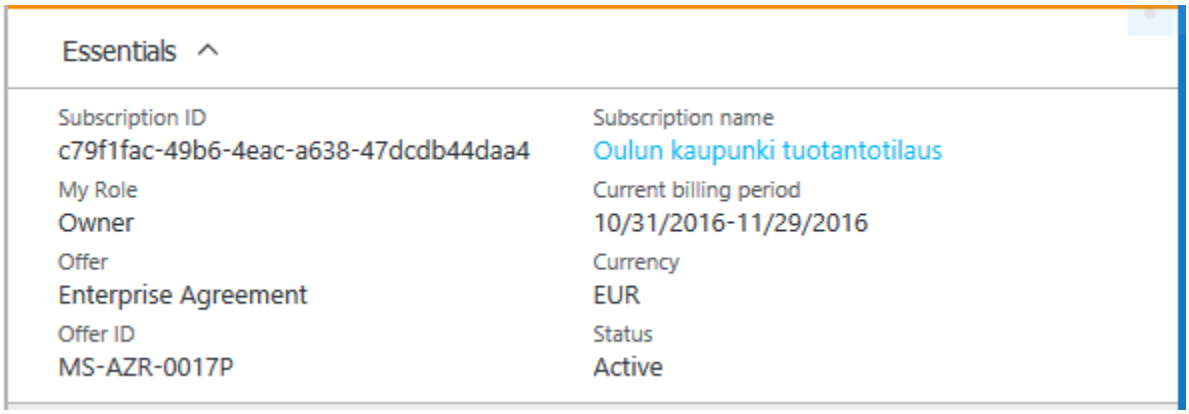
Tämä hakemisto tulee automaattisesti mukaan kaikkiin uusiin tilauksiin, kun tilaukset perustetaan käyttämällä edellä mainittua xxx -käyttäjätunnusta.

Tuotantotilaukset on perustettu (ja mahdolliset testi- ja kehitystilaukset perustetaan) Oulun Kaupungin EA-(Enterprise Agreement) sopimuksen alle, jolloin niiden aiheuttamat kustannukset kohdistetaan EA-sopimukseen hankittavalle Azure Commitmentille. Ohessa kuva Azuren tilausrakenteesta:



2.1 Tuotantotilaus

Oukan Azure-tuotantotilauksen tiedot ovat:



2.2 Testi- ja kehitystilaukset

Kuten edellä on todettu, mahdolliset testi- ja kehitysympäristöt pyritään perustamaan omiin Azure-tilauksiinsa. Myös nämä testi- ja kehityskäyttöön tarkoitetut Azure-ympäristöt perustetaan Oukan EA-sopimuksen alaisuuteen.

2.3 Tilausten perustaminen

Tuotantotilaukset on perustettu käyttämällä käyttäjätunnusta xxx. Tilausten perustaminen ja hallinta tapahtuu käyttämällä Azuren hallintaportaalia https://portal.azure.com.

2.4 Azure-komponenttien sijainti

Azure-tilauksen puitteissa erilaisia resursseja ja objekteja voidaan perustaa mihin tahansa Azure-konesaliin, mutta on huomattava, että kaikki virtuaaliverkot on perustettu West Europe -konesaliin (konesali sijaitsee Amsterdamissa Hollannissa), ja näin ollen kaikki virtuaaliverkkoihin liittyvät resurssit on myös perustettava West Europe -konesaliin. Lähtökohtaisesti myös kaikki muut Azureen perustettavat resurssit perustetaan West Europe -konesaliin. Tästä voidaan tarvittaessa poiketa, mutta ainoastaan erityistapauksissa.

2.5 Tilausten hallinta

Kaikkien Oukan EA-sopimuksen alle luotujen tilausten hallinta tapahtuu Azuren EA-porttaalissa https://ea.azure.com. Tähän porttaaliin on tarvittavat käyttäjäoikeudet digi:n pääkäyttäjillä. EA-porttaalin kautta voidaan esim. seurata tilausten generoimaa laskutusta.

2.6 Azure-toimintojen hallinta

Tilausten sisältämiä resursseja ja toimintoja voidaan hallita käyttämällä jotain kolmesta eri menetelmästä:

- Azuren hallintaportaali https://portal.azure.com. Tätä hallintakäyttöliittymää käytetään ensisijaisesti kaikkien resurssien perustamiseen ja hallintaan.
- Azuren PowerShell-komentoliittymä. Lisätietoja PowerShell-komentojen asentamisesta ja käytöstä löytyy osoitteesta https://docs.microsoft.com/en-us/powershell/azureps-cmdlets-docs/.

3 Perusmääritykset

3.1 Azureen luotavien resurssien nimeämiskäytäntö

Azureen luotavien resurssien nimeämisessä käytetään seuraavanlaista nimeämiskäytäntöä:

<resurssin tyyppi>-<omistajatunniste>-<käyttötarkoitus>

missä

<resurssin tyyppi> on Azureen perustettavan resurssin tyyppi:

- RG tarkoittaa resurssiryhmää (Resource Group)
- VM tarkoittaa virtuaalipalvelinta (Virtual Machine)
- sa tarkoittaa tallennustiliä (Storage Account, storage accounttien nimissä kaikkien kirjaimien on oltava pieniä kirjaimia)
- VNet tarkoittaa virtuaaliverkkoa (Virtual Network)
- jne.

<omistajatunniste> on perustettavan resurssin omistaja eli asiakasorganisaatio:

- Ouka tarkoittaa Oulun kaupungin yleisiä resursseja
- Siku tarkoittaa Sivistys- ja kulttuuritoimea

<käyttötarkoitus> korvataan käyttötarkoitusta kuvaavalla tunnisteella, esim. Prod (tuotantoresurssi) tai Test/dev (testikäytössä oleva resurssi).

Esimerkkejä nimistä:

- RG-Ouka-VM-Prod – Oulun kaupungin yleisiä tuotantokäytössä olevia virtuaalipalvelimia varten perustettu resurssiryhmä.
- VNet-Siku-Prod – Sivistys- ja kulttuuritoimen tuotantokäytössä oleva virtuaaliverkko.

3.2 Resource Group -määritykset

Kukin perustettava resurssi sijoitetaan johonkin resurssiryhmään (Resource Group). Näitä resurssiryhmiä käytetään kahteen tarkoitukseen:

1. Laskutustiedon tallentamiseen – Azuren kulutus- ja laskutustiedot kerätään Oukan laskutusjärjestelmään, jossa resurssien aiheuttamat kustannukset kohdistetaan organisaatioyksiköihin resurssiryhmien perusteella. Kunkin resurssiryhmän perustamisessa ja nimeämisessä pitää tämän vuoksi noudattaa erityistä huolellisuutta.
2. Käyttöoikeuksien määrittämiseen – Azuren hallintaoikeudet voidaan tarvittaessa määrittää resurssiryhmäkohtaisesti niin, että jollakin pääkäyttäjällä voi olla oikeus hallita ainoastaan kyseiseen reusrssiryhmään kuuluvia resursseja.

Azuren subscriptioneja suunniteltaessa on huomioitava varsinkin 980 resurssiryhmän rajoite per tilaus joka rajoittaa sitä miten tilauksia ja niiden resurssiryhmiä suunnitellaan.

Alustava sovellusmäärä huomioiden suunnittelun lähtökohtana on käytetty tietoa että kaikki sovellukset ja niiden tarvitsemat komponentit sekä resurssiryhmät mahtuvat yhteen Azure-tuotantotilaukseen. Mikäli applikaatiomäärät kasvavat voidaan rinnalle perustaa uusia tilauksia tarpeen mukaan.

Resurssiryhmän nimen lisäksi resurssiryhmän omistajatieto voidaan tallentaa resurssiryhmään myös ns. Tagin muodossa. Tagit ovat avain:arvo-pareja, joihin voidaan tallentaa tieto esimerkiksi resurssiryhmän omistavasta organisaatioyksiköstä (Osasto: Siku). On huomattava, että yhdellä resurssiryhmällä (tai resurssilla) voi olla enintään 15 tagia.

Uutta tilausta luotaessa on hyvä kiinnittää huomiota myös resurssin tarjoajiin (resource providers). Kun uusi Azure tilaus on luotu siihen on otettu käyttöön vain tietyt perus resurssin tarjoajat. Kun lähdetään luomaan resurssia jota ei tilaukseen ole aiemmin luotu, tarvitaan resurssin tarjoajan rekisteröinti johon ei oletuksena resurssiryhmän omistajalla riitä oikeudet vaan oikeuksia pitää olla tilaus tasolla. Tästä syystä on hyvä rekisteröidä tietyt resurssin tarjoajat joiden tarve on tunnistettu jo etukäteen.

3.3 Storage Account -määritykset

Kaikki Azureen tallennettava tieto tallennetaan Azuren tallennusjärjestelmään. Tallennusjärjestelmässä kaikki tallennettava tieto ryhmitellään tallennustilien (Storage Account) alle. Näitä Storage Accountteja voi olla yhdessä tilauksessa enimmillään 250 kappaletta, joten Accounttien määrittämisessä pitää olla erityisen huolellinen. Kullekin Storage Accountille määritetään seuraavat ominaisuudet:

- Sijoituspaikka (lähtökohtaisesti West Europe, eli Amsterdamin konesali)
- Replikointi – oletuksena käytetään LRS-tallennustyyppiä (Locally Redundant Storage), mikä tarkoittaa, että kaikki Storage Accountin alle tallennettava tieto tallennetaan yhteen konesaliin (West Europe), mutta kolmeen erilliseen levyyn. Tarvittaessa voidaan käyttää myös GRS-tallennustyyppiä (Geo-Redundant Storage), mikä tarkoittaa, että tallennettava tieto replikoidaan myös toiseen konesaliin (West Europe -konesalin pari on North Europe, eli Dublinin konesali). Tällöin tieto tallennetaan kumpaankin konesaliin kolmeen erilliseen levyyn.
- Tallennustyyppi – General Purpose tai Blod Storage, jälkimmäistä käytetään, jos halutaan hyödyntää Cool Storage -tallennustilaa (tarkoitettu kerran kirjoitettavalle tiedolle, jota luetaan harvoin, jos koskaan).
- Tiedon salaus tallennettaessa

Nämä kaikki määritykset ovat Storage Account -kohtaisia, mikä tarkoittaa, että erilaisia käyttötarkoituksia varten perustetaan oma Storage Account. Lisäksi Storage ACcountteja joudutaan perustamaan myös yhden Storage ACcountin ruosituskykyrajoitusten vuoksi. Kannattaa kuitenkin huomioida edellä mainittu 250 Storage Accountin maksimirajoitus, mikä tarkoittaa, että Storage ACcounttien käyttö pitää tarkoin suunnitella.

3.4 Käyttöoikeusmääritykset

Azure-ympäristön hallintaan voidaan antaa joko koko tilauksen kattavia pääkäyttöoikeuksia, tai oikeudet voidaan tarvittaessa rajoittaa yhteen yksittäiseen resurssiin tai resurssiryhmään. Resurssi- tai resurssiryhmäkohtaisia käyttöoikeuksia voidaan lisäksi määrittää hyvin tarkasti roolipohjaisesti.

Tällä hetkellä Oukan tuotantotilauksessa on seuraavat tilaustason pääkäyttäjät:

XXX

Muita pääkäyttöoikeuksia määritetään tarpeen mukaan.

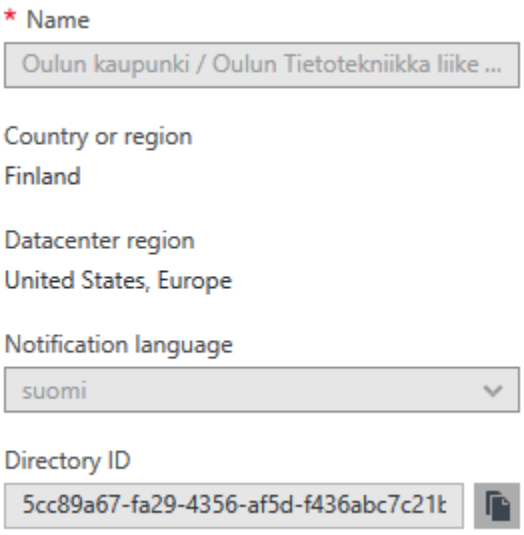
Azure tilauksen resurssiryhmä -tasolla annettavat oikeudet määräytyvät applikaation omistajan mukaan. Kun asiakkaalle luodaan resurssiryhmä Oukan toimesta, lisätään resurssiryhmän omistajaksi (owner) applikaation omistaja. Tämä kyseinen applikaation omistaja voi lisätä resurssiryhmään muita jäseniä ja luoda siihen applikaation tarvitsemia resursseja.

Laskutuksen kannalta oleellista on ettei applikaation omistaja pääse poistamaan kyseistä resurssiryhmää vaan että resurssiryhmien luonti ja poisto on Oukan vastuulla. Tätä voidaan hallita käyttöoikeuksien hallinnalla tai resurssien lukitsemisilla.

4 Azure AD -hakemisto

Azure-tilauksessa käytettäviä käyttäjätunnuksia varten Azure-tilaukseen on liitetty Azure AD -hakemisto, joka on alun perin luotu Oukan Office 365 -ympäristöä varten. Hakemisto tulee kaikkiin jatkossa perustettaviin tilauksiin, kunhan ne perustetaan käyttämällä samaa kohdassa 2.3. dokumentoitua käyttäjätunnusta. Eri asiakkaiden spesifisiin tilaukseen tehdään oma hakemisto jotta saadaan eriytettyä käyttäjienhallinta omakseen.

Azure AD -hakemiston tenanttitunnus on oulunkaupunki.onmicrosoft.com (hakemisto-ID: 5cc89a67-fa29-4356-af5d-f436abc7c21b) ja hakemiston tiedot ovat:



Azure AD -hakemisto on synkronoitu Oukan paikallisen AD:n kanssa ja siihen on määritetty seuraavat domainnimet:

XXX

Hakemistossa olevia käyttäjätunnuksia käytetään sekä Azure-tilausten pääkäyttäjien tunnuksina, sekä soveltuvin osin myös eri Azure-resurssien käyttäjätunnuksina.

4.1 Tilauksissa käytettävä Azure AD -hakemisto

Kun ympäristöön luodaan uusia Azure-tilauksia testi- ja kehityskäyttöön, on tilaus syytä luoda käyttämällä kohdassa 2.3. määritettyä käyttäjätunnusta, jotta kaikkiin tilauksiin tulee automaattisesti mukaan em. Azure AD -hakemisto. Kaikkien tilausten pääkäyttäjätunnukset määritetään tästä hakemistosta.

4.2 Paikallinen Active Directory -hakemisto

Oukan Azure-tilaukseen liitettävän Azure AD -hakemiston lisäksi tilaukseen yhdistetään myös Oukan paikallinen AD-hakemisto. Tätä varten Oukan tuotantotilaukseen tuodaan kaksi paikallisen AD-ympäristön Domain Controller -palvelinta, jotka toimivat myös tuotantotilauksen virtuaaliverkkoihin määritettävinä DNS-palvelimina. Paikalliseen AD-ympäristöön määritetään oma Site Azure-virtuaaliverkkoja varten.

4.3 Tilaustason pääkäyttäjien määritys

Kuhunkin tilaukseen määritetään joukko tilaustason pääkäyttäjiä. Näillä tunnuksilla on kaikki oikeudet kaikkiin tilauksen alle perustettaviin resursseihin. Tilauksen pääkäyttäjät määritetään Azuren vanhan hallintaporttaalin (https://manage.windowsazure.com) kautta valitsemalla porttaalin vasemmasta valikosta Settings (vasemman valikon alimmainen vaihtoehto) ja sen jälkeen sivun ylälaidasta Administrators-välilehti:

xxx

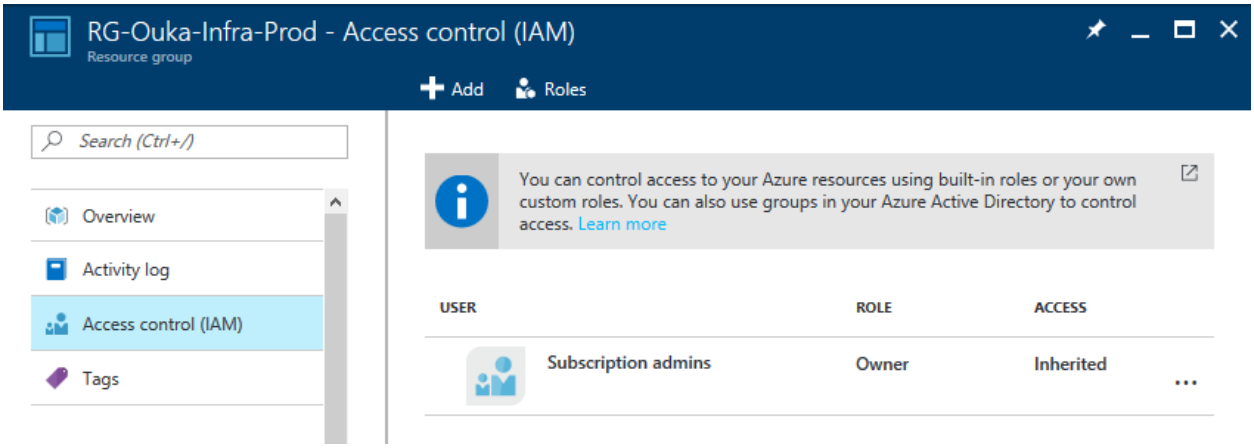
Tällä hetkellä Azure-tuotantotilaukseen on määritetty seuraavat tilaustason pääkäyttäjät:

xxx

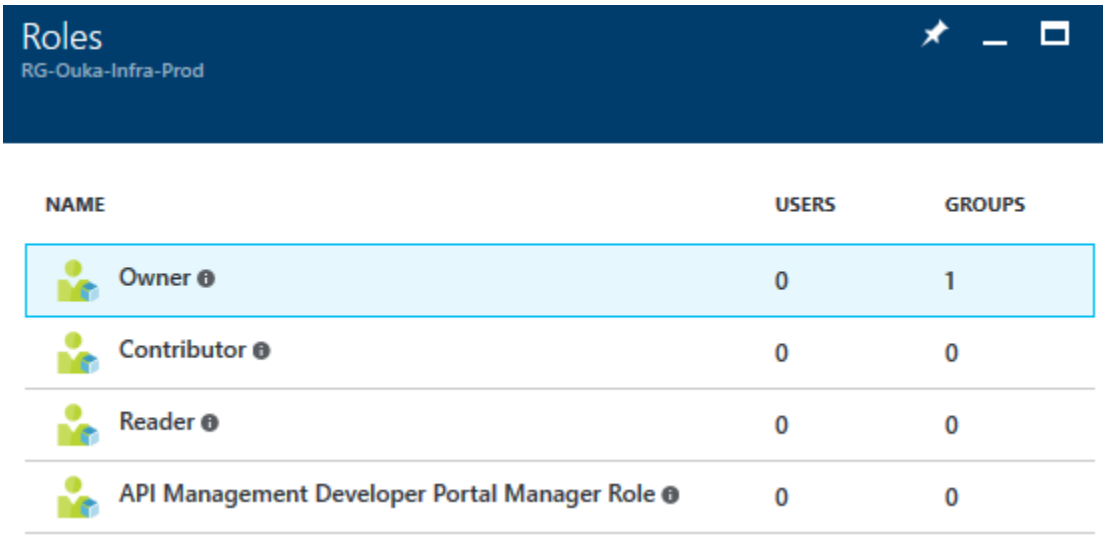
Tuotantotilauksessa on tarkoitus, että tilaustason pääkäyttäjiksi määritetään digi:n ylläpitohenkilöitä. Testi- ja kehitystilausten tilaustason pääkäyttäjiksi voidaan määrittää tarvittaessa myös eri yksiköiden käyttäjiä. Kaikkien tilausten pääkäyttäjätunnukset määritetään tilauksen yhteyteen tuotavasta Azure AD -hakemistosta oulunkaupunki-onmicrosoft.com.

4.4 RBAC-pääkäyttöoikeudet

Tilaukseen määritettäville resursseille voidaan tarvittaessa määrittää pääkäyttäjiä myös yksittäisille resursseille tai resurssiryhmille. Määritys tehdään Azure-tilauksessa käyttämällä uutta hallintaporttaalia (https://portal.azure.com). Kunkin resurssin tai resurssiryhmän alla on vaihtoehto Access control (IAM), jonka avulla resurssille tai resurssiryhmälle voidaan määrittää omat käyttöoikeudet käyttäjä- tai käyttäjäryhmäkohtaisesti:



Käyttäjät ja ryhmät tulevat tilaukseen liitetystä Azure AD -hakemistosta. Käyttäjille tai ryhmille voidaan määrittää joko kaikki oikeudet kyseiseen resurssiin tai resurssiryhmään (Owner-rooli), tai oikeuksia voidaan rajoittaa käyttämällä muita kuin Owner-rooleja (esim. Contributor tai Reader):



Azureen on valmiiksi määritetty joukko rooleja, ja lisäksi rooleja voidaan määrittää myös tarkemmin käyttämällä PowerShell-komentoja.

5 Hallintamenetelmät

Azure-ympäristön hallintaan voidaan käyttää useita eri menetelmiä esim Azure hallintaportaalia:

- Hallintaporttaali sijaitsee osoitteessa https://portal.azure.com. Hallintaporttaali hyödyntää Azure Resource Model -objektimallia (ARM), ja lisäksi se tukee resurssiryhmien sekä resurssiryhmille tai yksittäisille resursseille määritettäviä käyttöoikeuksia. Portaalin avulla voidaan määrittää ja hallita lähes kaikkia Azureen määritettäviä resursseja.

Lisäksi Azuren hallintatoimia voidaan tehdä myös PowerShell-komentoliittymän kautta. Kaikki hallintamenetelmät ovat käytettävissä kaikilla käyttäjätunnuksilla, joille on annettu hallintaoikeuksia Azure-tilaukseen (sekä tilaustason oikeudet että tarkemmat resurssi- tai resurssiryhmäkohtaiset oikeudet).

Lisätietoja eri hallintamenetelmien käytöstä on pääkäyttäjädokumentaatiossa.

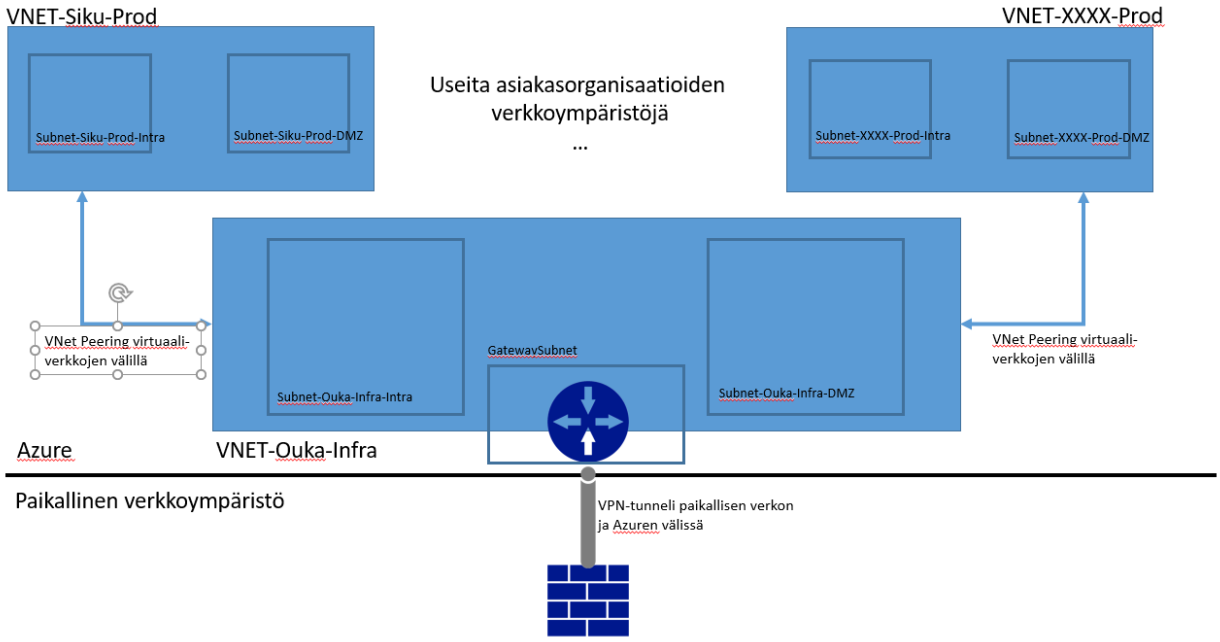
6 Verkkomääritykset

Tässä dokumentissa käsitellään ainoastaan Oukan Azure-tuotantotilaukseen tehtyjä ja tehtäviä verkkomäärityksiä. Sovellus tai asiakaskohtaiset, testi- tai kehitystilauksiin tehtävät verkkomääritykset dokumentoidaan erikseen tapauskohtaisesti. Pääsääntöisesti sovelluskohtaiset tilaukset käyttävät azuren julkisia verkkomäärityksiä ja tämän dokumentin sisältäviä virtuaaliverkkomäärityksiä ei tarvitse käyttää.

6.1 Yleistä verkkomäärityksistä

Oukan Azure-tuotantotilaukseen on määritetty useita virtuaaliverkkoja, joihin sijoitetaan sekä yhteisiä virtuaalikoneita että asiakasorganisaatioiden virtuaalikoneita. Yhteisiä, yleisessä käytössä olevia virtuaalikoneita varten on oma virtuaaliverkkonsa (VNET-Ouka-Infra) ja kutakin asiakasorganisaatiota varten luodaan oma virtuaaliverkko (esim. VNET-Siku-Prod). Nämä virtuaaliverkon on edelleen jaettu aliverkkoihin.

Yleisestä VNET-Ouka-Infra-virtuaaliverkosta on muodostettu VPN-yhteys Oukan paikalliseen verkkoympäristöön ja lisäksi virtuaaliverkot on yhdistetty toisiinsa. Seuraavassa kuvassa on esitetty verkkojen rakenne:



6.2 Virtuaaliverkot ja aliverkot

Kukin virtuaaliverkko jaetaan kahteen osaan, joita käytetään seuraavasti:

- Intra-aliverkko – tänne sijoitetaan kaikki palvelimet, joihin ei tarvita verkkoyhteyttä suoraan Internetistä ja joista pitää voida kommunikoida Oukan paikalliseen verkkoon.
- DMZ-aliverkko – tänne sijoitetaan kaikki palvelimet, joihin tarvitaan verkkoyhteys Internettiin. DMZ-verkosta ei lisäksi voi kommunikoida suoraan Oukan paikalliseen verkkoon, vaan kaikki liikenne sinne on mentävä jonkin Intra-verkossa olevan palvelimen kautta.

Azure-tuotantoympäristöön on määritetty esim. seuraavat virtuaaliverkot:

Verkko	Käyttötarkoitus
VNET-Ouka-Infra	Ympäristön yhteiset, kaikissa virtuaaliverkoissa käytettävät palvelimet ja palvelut (esim. DC:t ja DNS-palvelimet)
VNET-Siku-Prod	Sivistys- ja kulttuuritoimen palvelimet

Virtuaaliverkkoja perustetaan tarvittaessa lisää, kutakin asiakasorganisaatiota varten omansa.

Virtuaaliverkoissa käytetään seuraavia IP-osoiteavaruuksia:

Verkko	IP-avaruus
VNET-Ouka-Infra	xxx
VNET-Siku-Prod	xxx

Virtuaaliverkko VNET-Ouka-Infra on jaettu kolmeen aliverkkoon:

Aliverkko	Osoiteavaruus	Huomautuksia
Subnet-Ouka-Infra-Intra	xxx	Tähän aliverkkoon sijoitetaan kaikki tuotantopalvelimet, joihin ei tarvita yhteyttä Internettiin ja/tai joista pitää pystyä kommunikoimaan Oukan paikalliseen verkkoon.
Subnet-Ouka-DMZ-Prod	xxx	Tähän aliverkkoon sijoitetaan kaikki tuotantopalvelimet, joihin tarvitaan yhteys Internettiin. Näistä palvelimista ei voi kommunikoida suoraan Oukan paikalliseen verkkoon.
GatewaySubnet	xxx	Tämä aliverkko on varattu vain gateway-toimintoa varten.

Virtuaaliverkko VNET-Siku-Prod on jaettu kahteen aliverkkoon:

Aliverkko	Osoiteavaruus	Huomautuksia

Subnet-Siku-Intra	xxx	Tähän aliverkkoon sijoitetaan kaikki tuotantopalvelimet, joihin ei tarvita yhteyttä Internettiin ja/tai joista pitää pystyä kommunikoimaan Oukan paikalliseen verkkoon.
Subnet-Siku-DMZ	xxx	Tähän aliverkkoon sijoitetaan kaikki tuotantopalvelimet, joihin tarvitaan yhteys Internettiin. Näistä palvelimista ei voi kommunikoida suoraan Oukan paikalliseen verkkoon.

6.3 Azuren ja Oulun kaupungin paikallisen verkon välinen yhteys

Azuressa olevan VNET-Ouka-Infra-virtuaaliverkon ja Oukan paikallisen verkon välille on muodostettu Site-to-Site VPN -yhteys seuraavasti:

- VNET-Ouka-Infra-virtuaaliverkon aliverkossa GatewaySubnet on Azuren pään gateway (VNETGW-Ouka-Prod). Tällä gatewayllä on seuraavat tiedot:
    - VPN Gatewayn tyyppi: Route-Baed (IKEv2)
    - Azuren pään julkinen osoite: xxx
- Oukan päähän on sijoitettu palomuurilaite, johon VPN-yhteys päätetään:
    - Palomuurilaitteen tyyppi: ????
    - Oukan pään julkinen osoite: xxx
    - Asetukset: (tähän kopio VPN:n asetuksista)
- Azuren päähän on määritetty Loca Network Gateway LocalnetGW-Ouka-Prod:
    - Kohdeosoite: xxx
    - Osoiteavaruus:

Tässä yhteydessä on huomioitava ettei Sovelluskohtaisten tilauksien ja Oukan paikallisen verkon välillä ole mitään kytköksiä vaan Sovelluksen vaatimaan tilaukseen mahdollisesti rakennettavat virtuaaliverkot ovat täysin irrallaan Oukan ympäristöstä. On myös huomioitava tietoturva: Sovelluskohtaiset ratkaisut vaativat oman tietoturvarakenteen koska ne eivät sijaitse lähtökohtaisesti Oukan keskitettyjen tietoturvakomponettien takana.

6.4 Palvelimien sijoittelu eri virtuaaliverkkoihin ja niissä sijaitseviin aliverkkoihin

Kukin virtuaaliverkko on jaettu useaan aliverkkoon siksi, että eri aliverkoilla on erilaiset ominaisuudet:

- Intra-aliverkko on tarkoitettu palvelimille, joista
    - ei liikennöidä suoraan Internettiin (liikenne aliverkosta ohjataan Oukan sisäverkkoon)
    - voidaan liikennöidä Oukan sisäverkkoon.
- DMZ-aliverkko on tarkoitettu palvelimille, joista
    - liikennöidään suoraan Internettiin (palvelimista joko tarjotaan palveluja suoraan Internettiin tai niihin pääsee muuten suoraan Internetistä kiinni).

Nämä verkkomääritykset ja -rajoitukset toteutetaan käyttämällä Network Security Grouppeja (NSG) ja routing-tableja.

6.5 DNS-määritykset

Oukan Azuren tuotantotilauksessa kunkin virtuaaliverkon DNS-määritykset määritetään niin, että verkkojen DNS-palvelimet ovat Azuressa VNet-Ouka-Infra-verkossa sijaitsevat kaksi DNS-palvelinta. Näistä kahdesta DNS-palvelimesta edelleenohjataan DNS-kyselyt Oukan sisäverkossa oleville DNS-palvelimille (DNS Forwarding).

Sovelluskohtaisessa tilauksessa jokainen sovellus vastaa itse mahdollisen virtuaaliverkon DNS tarpeista.

6.6 Verkkojen Network Security Group -määritykset

Oukan Azure-tilauksessa kuhunkin aliverkkoon määritetään Network Security Group -objektit (NSG), joilla rajoitetaan, mihin verkosta voidaan liikennöidä ja millä protokollalla.

6.7 Verkkoyhteyksien valvonta

7 Virtuaalikonemääritykset

7.1 Palvelinten Storage Account -määritykset

Kunkin asiakasorganisaation virtuaalipalvelimille määritetään omat Storage Account -määritykset. Storage Accounttien määrityksessä on huomioitava Storage Account -rajoitukset (kts. kohta 3.3).

7.2 Uuden virtuaalikoneen luonti

7.3 Palvelimen verkkomääritykset

Kukin virtuaalipalvelin sijoitetaan omistavan organisaatioyksikön virtuaaliverkossa siihen aliverkkoon, joka parhaiten soveltuu palvelimen käyttötarkoitusta varten (intra-aliverkko tai DMZ-aliverkko). Yhdellä palvelimella voi olla useita verkkoliittymiä (Network Interface, 1 – 4 kpl per palvelin, määrä riippuu palvelimen koosta) sekä useita IP-osoitteita (sisäisiä tai julkisia IP-osoitteita).

7.3.1 Sisäiset verkko-osoitteet

Kukin palvelin saa sisäisen verkko-osoitteensa siitä virtuaaliverkosta ja aliverkosta, johon se sijoitetaan. Kaikkien palvelimien IP-osoitteet myönnetään palvelimille DHCP:n avulla. Palvelimiin ei saa määrittää kiinteitä IP-osoitteita palvelimien käyttöjärjestelmästä. Jos palvelimelle tarvitaan ”kiinteä” IP-osoite, voidaan se tarvittaessa määrittää ”staattiseksi” (Static) Azuren hallintaliittymästä.

7.3.2 Julkiset verkko-osoitteet

DMZ-aliverkkoon sijoitettaville palvelimille voidaan määrittää myös julkinen IP-osoite (yksi tai useita). Jos palvelimelle määritetään julkinen IP-osoite, on se suojattava käyttämällä Network Security Group -määritystä.

7.3.3 Usean verkkokortin palvelin

Yhdellä palvelimella voi olla useita verkkoliittymiä (Network Interface, 1 – 4 kpl per palvelin, määrä riippuu palvelimen koosta) sekä useita IP-osoitteita (sisäisiä tai julkisia IP-osoitteita).

7.3.4 Palvelinten Network Security Group -määritykset

Yksittäiselle palvelimelle määritetään NSG ainoastaan siinä tapauksessa, että palvelimeen määritetään julkinen IP-osoite tai siinä on muuten erityisesti suojeltavia verkkoliittymiä. Muutoin kaikissa palvelimissa käytetään palvelimen omaa palomuuria suojaamaan ja suodattamaan verkkoliikennettä.

7.4 Palvelinten päivitys

Oukan Azure tilaukseen sijoitettavien Windows-palvelimien päivitys hoidetaan Azuressa olevan Windows Update -palvelimen välityksellä. Kaikki palvelimet liitetään ko. Windows Update -palveluun. Palvelimien päivityksiä valvotaan Operations Management Suite -palvelun välityksellä.

Sovelluskohtaisissa tilauksissa asiakkaat vastaavat itse palvelimiensa päivityksistä ja valvonnasta.

7.5 Palvelinten haittaohjelmien torjunta

Lähtökohta on, että Azureen sijoitettaviin Windows-palvelimiin määritetään haittaohjelmien torjunta. Haittaohjelmien torjuntajärjestelmänä käytetään System Center Endpoint Protection -järjestelmää, jota käytetään myös Oukan muissa palvelimissa. Palvelimien haittaohjelmien torjuntaa valvotaan SCEP-palvelimen ja Operations Management Suite -palvelun välityksellä.

Sovelluskohtaisissa tilauksissa asiakas vastaa itse palvelimiensa haittaohjelmien torjunnasta.

8 Varmistusmääritykset

Kaikki Azureen sijoitettavat Windows-palvelimet määritetään tarpeen mukaan Azuren varmistusjärjestelmän piiriin. Kullekin Oukan ja Business Oulun asiakasorganisaatiolle määritetään käyttöön oma Azure Backup Vault (Recovery Services Vault), jota käytetään ko. asiakasorganisaation varmistusten tallentamiseen (esimerkiksi Recvault-Siku-Prod on sivistys- ja kulttuuritoimen vault-tallennustila). Näiden asiakaskohtaisten vault-tallennustilojen lisäksi ympäristössä on myös yksi yleinen vault-tallennustila Recvault-Ouka-prod, jota käytetään yleisten, infrastruktuuriin liittyvien palvelimien varmistamiseen sekä lisäksi ympäristöön määritetyn Site Recovery -palvelun tallennustilana Oukan Azure tilauksessa.

Normaalin varmistuspalvelun lisäksi ympäristöön on määritetty Site Recovery -palvelu, jota käytetään paikalliseen VMWare-ympäristöön määritettyjen virtuaalipalvelimien varmistamiseen sekä palvelimien migraatioon paikallisesta ympäristöstä Azureen.

8.1 Azure Backup -palvelu

Palvelimista otetaan Snapshot-tyyyppiset varmistukset Azuren Backup-toiminnolla. SnapShot-päivityksiä varten Azureen määritetään tarvittava määrä Backup Policyjä, joissa määritetään kaksi asiaa:

- varmistuksen ottamisajankohta (päivittäinen/viikoittain, kellonaika)
- varmistuksen säilytysaika (päivittäisten, viikoittaisten, kuukausittaisten ja vuosittaisten varmistusten säilytysaika, Azuressa varmistuksia voidaan määrittää säilytettäviksi enintään 99 vuoden ajan).

Backup Policyt määritetään asiakaskohtaisesti. Useammassa palvelimessa voidaan käyttää samaa Backup Policyä.

Azure Backupin avulla otettuja SnapShot-varmistuksia voidaan palauttaa palvelinkohtaisesti (joko ”samaan” palvelimeen tai tyystin eri paikkaan), levykohtaisesti (ainoastaan PowerShell-komennoilla) tai SnapShotista voidaan palauttaa yksittäisiä tiedostoja (toiminto on vielä Preview-tilassa, toiminto on otettu käyttöön Oukan ympäristössä ja siitä on olemassa erilliset ohjeet).

8.2 Azure Site Recovery -palvelu

Oukan Azure tilauksen ja Oukan paikallisen ympäristön välille on määritetty Azure Site Recovery -palvelu. Site Recoveryn avulla paikallisessa VMWare-ympäristössä olevia palvelimia voidaan replikoida Azureen joko varmistus- tai migraatiotarkoituksessa, ja replikoinnin jälkeen siirtää palvelin suoritettavaksi Azureen.

Site Recovery -palveluun on määritetty seuraavat komponentit:

- Kaikki määritykset sijaitsevat yleisessä Recvault-Ouka-Prod-tallennustilassa.
- Paikalliseen VMWare-ympäristöön on asennettu toiminnon hallintapalvelin (COnfiguration Server):
    - Palvelimen nimi: xxx
    - IP-osoite: xxx
    - Hallintapalvelin on liitetty vCenter-palvelimeen xxx
- Hallintapalvelimella käytetään käyttäjätunnusta ”Asr Ouka Tili”, jonka avulla Azuressa tehdyt hallintatoiminnot välitetään vCenter-ympäristöön ja yksittäisille palvelimille.

8.2.1 Site Recoveryn komponentit

Site Reccovery -palvelua varten on määritetty seuraavat komponentit:

- Recovery Services Vault (Oukan yhteinen, kaikkeen varmistukseen ja migraatioon käytetään samaa Vaulttia)
- Control Service VMWare-ympäristössä.

9 Hallintatoiminnot

9.1 Operations Management -palvelu

Ympäristöön on luotu OMS-ympäristö OMS-Ouka-prod, jota on alkuvaiheessa tarkoitus käyttää kaikkien ympäristössä olevien palvelimien valvontaan. Jatkossa ympäristöön voidaan luoda muita, erillisiä OMS-ympäristöjä.

9.2 Resurssien hallinta Azure Policyn avulla

Azureen luotavia palveluita voidaan hallita Azure Policyn avulla. Normaaleja hallintakohteita ovat esimerkiksi lokaatiot joihin resursseja luodaan. Jotta resurssien luontilokaatiot olisivat linjassa verkkoarkkitehtuurin ja hallintapalveluiden kanssa (esim. Recovery Services Vault) on resurssit tärkeää pitää tietyissä Azuren lokaatioissa. Myös latenssit muuttuvat täysin erilaisiksi mikäli palvelut sijaitsevat kohtuuttoman pitkällä loppukäyttäjän näkökulmasta katsottuna.

Alkuvaiheessa Sovelluskohtaisissa Azure tilauksissa luodaan seuraavat Policyt:

- [policy] – [käyttötarkoitus]

  Näitä pitää viilata kovasti, jos halutaan välttää esim. ylisuurien koneiden asentaminen yms.

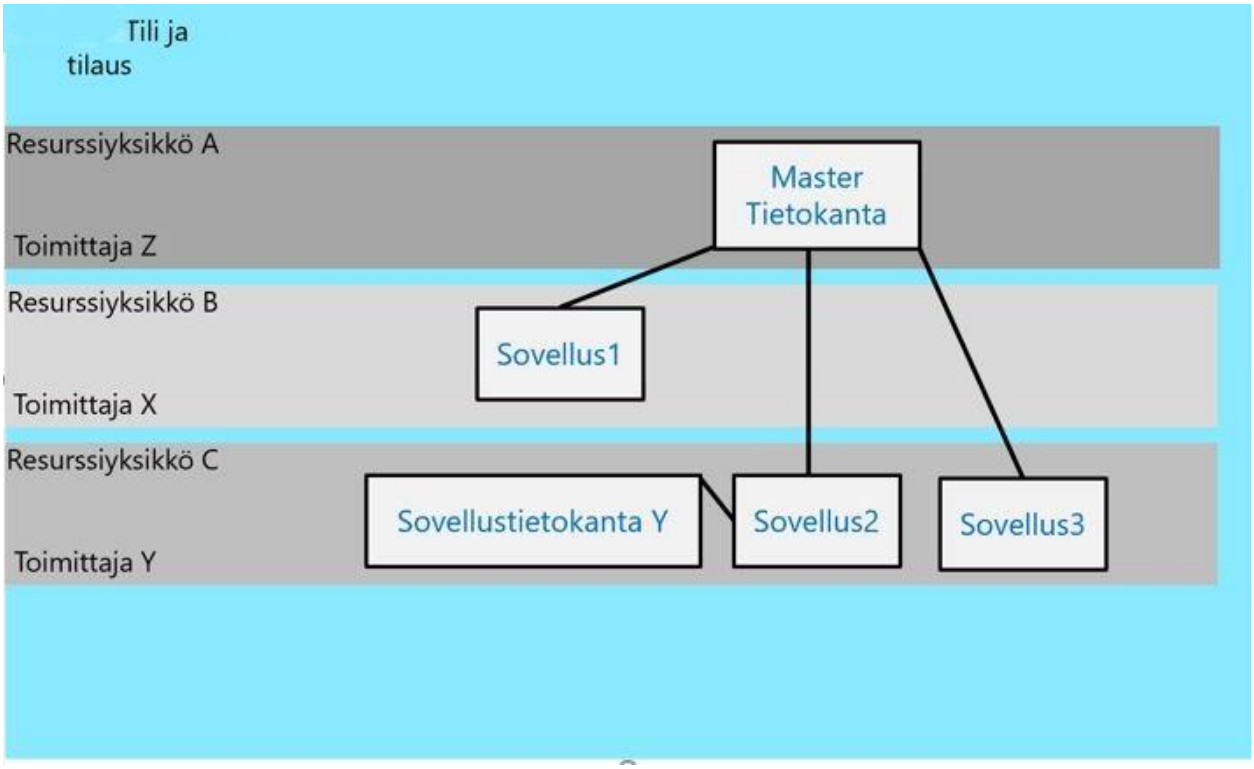
10 Tietoturva

10.1 Resurssipohjainen pääsynhallinta

Resurssipohjaisen pääsynhallinnan periaatteet on otettu mukaan suunniteltaessa Sovelluskohtaista Azure arkkitehtuuria. Käytännössä tämä tarkoittaa sitä että resurssiryhmiin (kuvassa Resurssiyksikkö) annetaan vain tarvittavat käyttöoikeudet sellaisille henkilöille joiden tarvitsee päästä hallitsemaan Azuressa sijaitsevia resursseja (Control Plane).

Itse resurssit juttelevat keskenään palvelutunnuksilla joille ei anneta oikeuksia Azuren portaalin puolella tapahtuvaan hallinnointiin vaan ainoastaan tarvittavat oikeudet päästä käsiksi tarvittavaan dataan (Data Plane). Tällöin esimerkiksi Sovellus 1 saa tarvittavat oikeudet Master Tietokanta -palveluun sellaisella tunnuksella jotta se pääsee hakemaan tarvitsemansa datan pienimmillä mahdollisilla oikeuksilla.

Näin suunniteltuna ja toteutettuna jokainen toimittaja voi hallita rakentamaansa palvelua omassa resurssiryhmässään ilman pääsyä toisen toimittajan toteuttamaan palveluun.


Tili ja
tilaus
Resurssiyksikkö A
Toimittaja Z
Master
Tietokanta
Resurssiyksikkö B
Toimittaja X
Sovellus1
Resurssiyksikkö C
Toimittaja Y
Sovellustietokanta Y
Sovellus2
Sovellus3